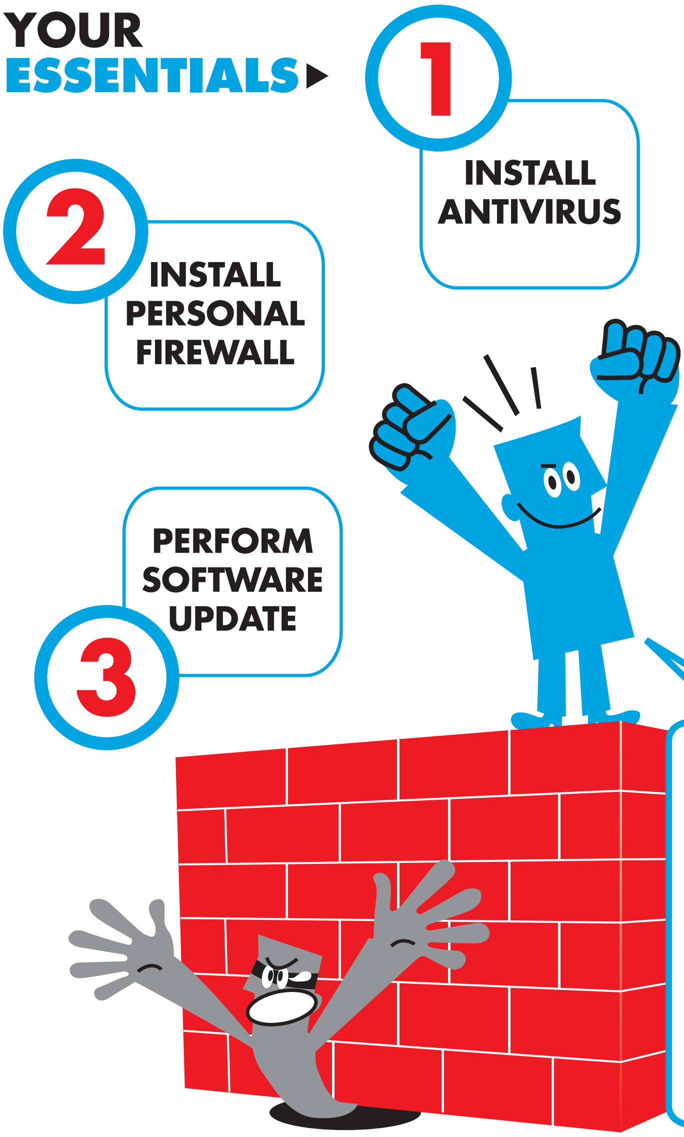
COMPUTER **SECURITY**

In the realm of cyber security, adopting appropriate security measures is critical in preventing your computer from being hijacked!

YOUR ESSENTIALS ▸



1 INSTALL ANTIVIRUS

2 INSTALL PERSONAL FIREWALL

3 PERFORM SOFTWARE UPDATE

ANTIVIRUS:

This is a software used to detect, stop and remove malware such as computer viruses, worm, Trojan horses, spyware, adware, etc from your computer.

SOFTWARE UPDATE:

Most operating system and software manufacturers release new updates upon discovery of vulnerabilities or bugs. Keep your software updated with the latest software patches.

PERSONAL FIREWALL:

This is a software that monitors network activities and blocks malicious traffic to and from your computer.

USEFUL TIPS

- To ensure that your antivirus software is effective, set it to update the virus signature file automatically.
- Set your personal firewall to block suspicious network activities or alert you of such attempts and let you decide whether to allow the traffic to go through.
- To minimise software vulnerability, it is recommended to configure the installed software to update itself automatically when patches are made available.

CYBERSECURITY
AWARENESS DAY

MOBILE SECURITY

A mobile device is a hand held computing device that has an operating system (OS), where "Apps" and software can be installed for use.

Most hand held devices come equipped with Wi-Fi, Bluetooth and GPS capabilities, which allow connections to the Internet and other Bluetooth capable devices such as a microphone headset. Examples of mobile devices are handphone, tablet PC and laptops.

DO

1 USE PASSWORD AND ENCRYPTION TO PROTECT YOUR DATA

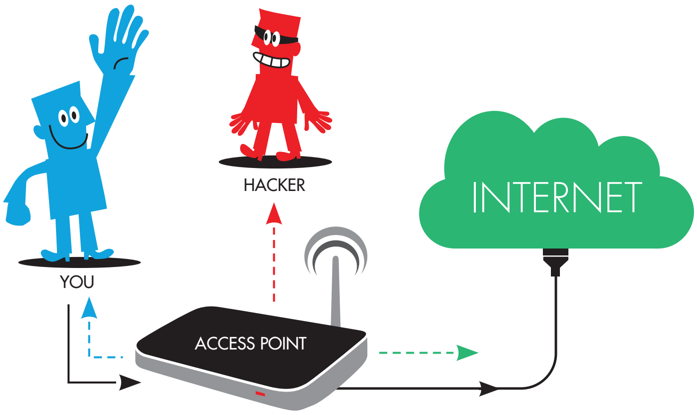
Password protect and turn on encryption for your mobile device to prevent unauthorised access to the data stored on your device.

2 DISABLE WIFI AND BLUETOOTH WHEN NOT IN USE

Attackers could access to information on your mobile device through its enabled WiFi or Bluetooth connection!

3 BACKUP DATA REGULARLY

In event that your mobile device's data is lost, you would be able to recover it!



DON'T

1 JAILBREAK/ROOT YOUR MOBILE DEVICE'S OPERATING SYSTEM

Jailbreaking/rooting might void your device's warranty and expose the operating system to vulnerabilities that could be exploited by hackers.

2 CONNECT TO UNKNOWN WIRELESS NETWORK

Hackers may setup unsecured WiFi hotspots in public area, once connected to it, they are able to intercept and steal sensitive data that you transmit over the Internet!

CYBERSECURITY
AWARENESS DAY

WIRELESS **SECURITY**

If someone is able to access your wireless connection, they may even be able to access the files on your computer.

Hackers may exploit your unsecured wireless network to compromise your computer or perform malicious activities in your name, such as sending spam emails or downloading illegal content.

AT HOME, secure your wireless network with the following settings:

ENABLE WPA2 ENCRYPTION WITH STRONG PASSPHRASE

Try to use a complex and long passphrase as your encryption key to ensure that your entire wireless setup is secure.

CHANGE THE DEFAULT WIRELESS ROUTER ADMINISTRATOR USERNAME AND PASSWORD

As with any password, make it a rule of thumb to have at least 8 alphanumeric characters in upper and lowercase, numbers and symbols for your password.

CHECK AND CONTROL THE DEVICES THAT ARE CONNECTED TO YOUR WIRELESS NETWORK

This can be done by checking the MAC address filtering settings.

DISABLE SSID BROADCAST

The SSID is essentially the name assigned to your network. SSID is broadcasted by your wireless router for devices to connect to your wireless network. You have the option to disable the broadcast if you do not want your wireless network name to be listed in devices' wireless network search.

IN OUTDOOR PLACES, protect your data privacy when using public Wi-Fi by practicing the following steps:

1 TURN OFF FOLDER SHARING

You would want to turn off sharing for your folders as anyone on the same network can access them. They don't even need to be a hacker.

2 AWARENESS IS GOOD PRACTICE!

Beware of the information you share in public locations. Even seemingly innocuous logins to Webmail accounts could give hackers access to your more important data, and especially since most people utilise the same password with a few variants for almost all online activities.

3 SWITCH IT OFF

If you are working offline for extended periods of time, shut down or disable your wireless connection. Every minute you're on someone else's wireless network is a minute you're exposing your machine and your data to intruders.

4 INVEST IN A GOOD ANTIVIRUS AND INTERNET SECURITY PRODUCT

Run a comprehensive security suite and keep it up to date to block out spyware and viruses.

CYBERSECURITY
AWARENESS DAY

ONLINE **SECURITY**

What is Online Identity?

An online identity is used to uniquely identify yourself to others online. Your personal data such as **NRIC, Internet banking login,** and **email address** could all be a form of your identity online.

Why do I need to secure my Online Identity?

If your personal data is disclosed online, malicious users could masquerade as you to conduct malicious acts. Your email address might be misused to send messages embedded with malware to your friends and associates or **funds might be taken out from your bank account.**

HOW TO PROTECT YOURSELF

LIMIT PERSONAL INFORMATION THAT YOU PUT ONLINE

Do not post/share personal information (e.g. Date of birth, phone number, etc) on websites as malicious users can easily harvest the information and misuse those information.

SAFE SURFING

Avoid entering sensitive information on unsecured sites. Install security suite (i.e. Anti-virus software and Firewall) on your surfing device.

SAFEGUARD YOUR PASSWORD

Do not share your password with others. As a good practise, use different passwords for different accounts. A strong password should be used and changed regularly to reduce its likelihood of being compromised.

WATCH OUT FOR PHISHING EMAILS

Do not reply to emails that requests for your personal information (e.g. password, credit card details).

CYBERSECURITY AWARENESS DAY